END USER'S GUIDE

VeriSign PKI Client Government Edition v 1.5

End User's Guide

VeriSign, Inc.

DISCLAIMER AND LIMITATION OF LIABILITY

VeriSign, Inc. has made efforts to ensure the accuracy and completeness of the information in this document. However,VeriSign, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein.VeriSign, Inc. assumes no liability to any party for any loss or damage (whether direct or indirect) caused by any errors, omissions, or statements of any kind contained in this document.

Further, VeriSign, Inc. assumes no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described herein do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described herein are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner. VeriSign Inc. reserves the right to make changes to any information herein without further notice.

TRADEMARKS

VeriSign, the VeriSign logo, VeriSign Intelligence and Control Services, VeriSign Trust Network, Go Secure!, OnSite, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Other trademarks and service marks in this document are the property of their respective owners.

This document supports Access for Managed PKI and all subsequent releases unless otherwise indicated in a new edition or release notes. This document may describe features and/or functionality that are not present in your software or your service agreement. Contact your account representative to learn more about what is available with this VeriSign product. If you need help using this product, contact customer support.

enterprise-pki-support@verisign.com

+1-650-426-3535 or 1-800-579-2848

Contents

1 Introduction

VeriSign PKI Client is software for digital signing, authentication, and data protection with desktop-based applications.

For digital signing, authentication and data protection, VeriSign PKI Client uses a Digital ID, a digital certificate, that represents and verifies your identity. This Digital ID is stored on a smart card or your computer.

There are many types of security devices that work with VeriSign PKI Client, including USB smart cards and biometric devices. For simplicity, this guide uses the term *smart card* for all for these devices.

Once you have received a Digital ID, you can use it for Windows login and with Outlook, Adobe Acrobat, and other Windows applications.

VeriSign PKI Client Features

VeriSign PKI Client offers the following features for Windows and Windows applications:

- **Secure Windows Login** - You can log on to your computer using a Digital ID stored on your smart card.
- **Computer Lock and Unlock** - You can lock and unlock your computer using the Digital ID stored on your smart card.
- **Secure Email** - Using a Digital ID stored on your smart card or computer you can digitally sign, encrypt, and decrypt email in Outlook.
- **Digital Signing of Documents** - Using a Digital ID stored on your smart card or computer you can digitally sign, encrypt, and decrypt documents in Adobe Acrobat and Microsoft Word.
- **SSL Web Authentication** - You can authenticate to web sites using an SSL Digital ID stored on your smart card or computer with Internet Explorer and Mozilla FireFox.

2 Installing VeriSign PKI Client

This section explains how to install VeriSign PKI Client on your computer.

System Requirements

The following are the hardware and software requirements for using VeriSign PKI Client. If you will be using VeriSign PKI Client with a smart card, such as a PIV or CAC, you will need a smart card reader.

Hardware Requirements

- Pentium III processor or newer
- 512MB RAM (memory)
- 5MB free hard drive space

Operating System Requirements

- Windows XP service pack 3 (32-bt)
- Windows Vista service pack 2
- Windows 7 (32- and 64-bit)
- Windows 2003 release 2 (32- and 64-bit)
- Windows 2008 release 2 (32- and 64-bit)

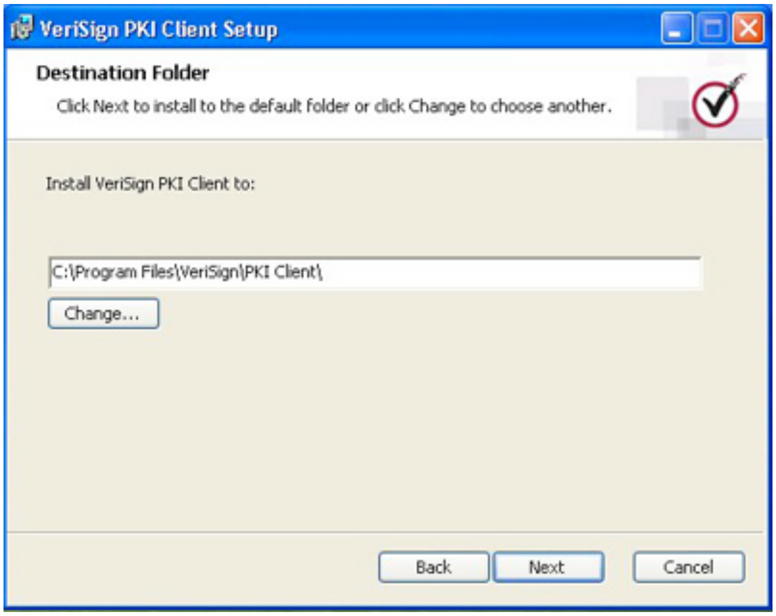
Smart Card Requirements

- A Personal Identity Verification (PIV) or Common Access Card (CAC) smart card
- A USB PC/SC compliant smart card reader
- The smart card reader manufacturer's drivers or support software

Installing VeriSign PKI Client with Microsoft Installer

To install VeriSign PKI Client on your computer, you will need to have local, administrator privileges on your computer.

1. Locate the VeriSign PKI Client installer, which will have been given to you as a file archive (.ZIP) or CD-ROM. If you were given a file archive, extract it to a folder on your computer. For example, *C:\Windows\TempVeriSign-PKI-Client*.
2. Double-click the installer, VeriSign-PKI-Client-x86-1.5.msi.
3. In the installer, click **Next**.



VeriSign PKI Client Setup

Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install VeriSign PKI Client to:

C:\Program Files\VeriSign\PKI Client\

Figure 2.1 - VeriSign PKI Client Installer

4. Read the End-User License Agreement, click the **I accept the terms in the License Agreement** box, and click **Next**.
5. Click **Next**.
6. Click **Install**.
7. Click **Finish**.

VeriSign PKI Client is now running. You can view it in the Windows notification area, also called the Windows tray (in the lower, right corner of your screen).

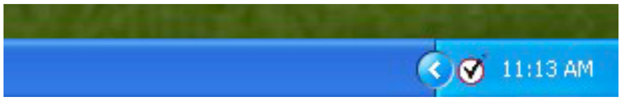
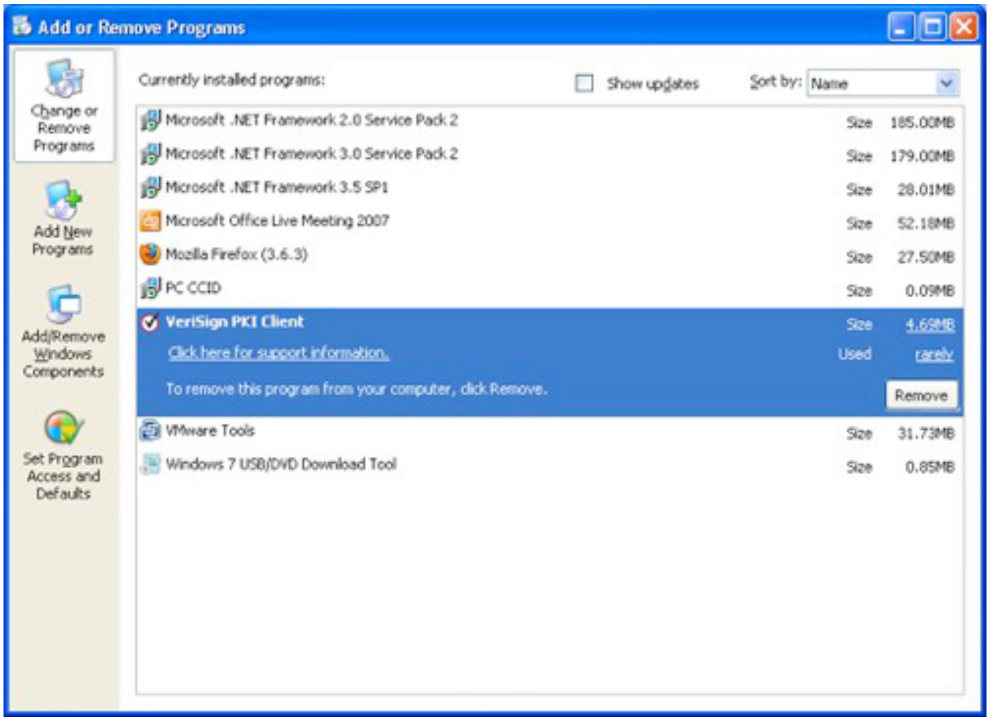


Figure 2.2 - VeriSign PKI Client Running

Un-installing VeriSign PKI Client

You may uninstall VeriSign PKI Client using the Control Panel:

1. Open the Control Panel (Start > Control Panel).
2. In the Control Panel, click **Add or Remove Programs**.
3. Select VeriSign PKI Client in the list of installed programs.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Remove

Currently installed programs: □ Show updates Sort by: Name

Microsoft .NET Framework 2.0 Service Pack 2	Size	185.00MB
Microsoft .NET Framework 3.0 Service Pack 2	Size	179.00MB
Microsoft .NET Framework 3.5 SP1	Size	28.01MB
Microsoft Office Live Meeting 2007	Size	52.18MB
Mozilla Firefox (3.6.3)	Size	27.50MB
PC CCID	Size	0.09MB
VeriSign PKI Client	Size	4.69MB
Click here for support information.	Used	rarely
To remove this program from your computer, click Remove.		Remove
VMware Tools	Size	31.73MB
Windows 7 USB/DVD Download Tool	Size	0.85MB

Figure 2.3 – Uninstall

4. Click **Remove**.
5. When prompted to confirm removal of VeriSign PKI Client, click **Yes**.

3 Using PKI Client

VeriSign PKI Client automatically runs when you start Windows and is displayed in the notification area.

Right-click the VeriSign check icon for the application menu.

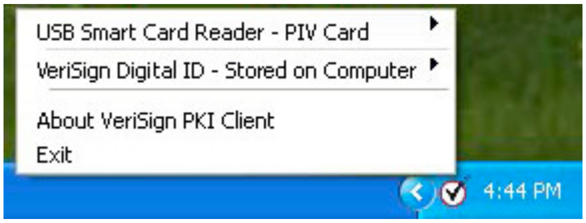

USB Smart Card Reader - PIV Card
VeriSign Digital ID - Stored on Computer
About VeriSign PKI Client
Exit
4:44 PM

Figure 3.1 - VeriSign PKI Client Menu

From this menu you can view and manage your Digital IDs, which is explained in the next section, *4. Managing Smart Cards and Digital Certificates*. You can also view information about the version of VeriSign PKI Client you are using.

Exiting VeriSign PKI Client

You can exit or quit VeriSign PKI Client from the notification area:

1. In the notification area, right-click the VeriSign PKI Client icon.
2. Select **Exit**.

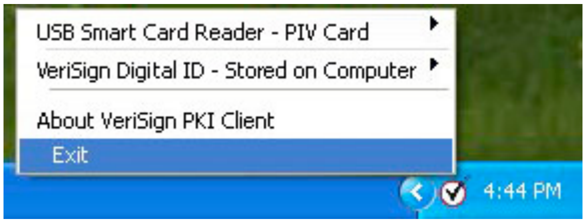

USB Smart Card Reader - PIV Card
VeriSign Digital ID - Stored on Computer
About VeriSign PKI Client
Exit
4:44 PM

Figure 3.2 - Exit VeriSign PKI Client

VeriSign PKI Client allows you to view the Digital IDs stored on your smart card or computer. Your Digital IDs are automatically added to the Windows certificate store, which is used by Windows and other applications, like Microsoft Outlook.

Viewing a Digital ID

You can view information about your Digital ID from the notification area. For example, you may view more information about the Digital ID, also called certificate, that is used for Authentication:

1. In the Windows notification area, right-click the VeriSign PKI Client icon.

2. In the menu, select the smart card or Digital ID.

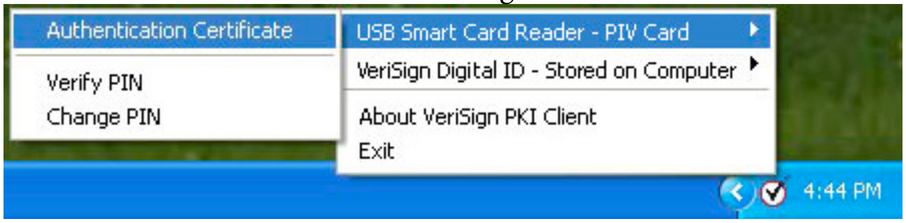
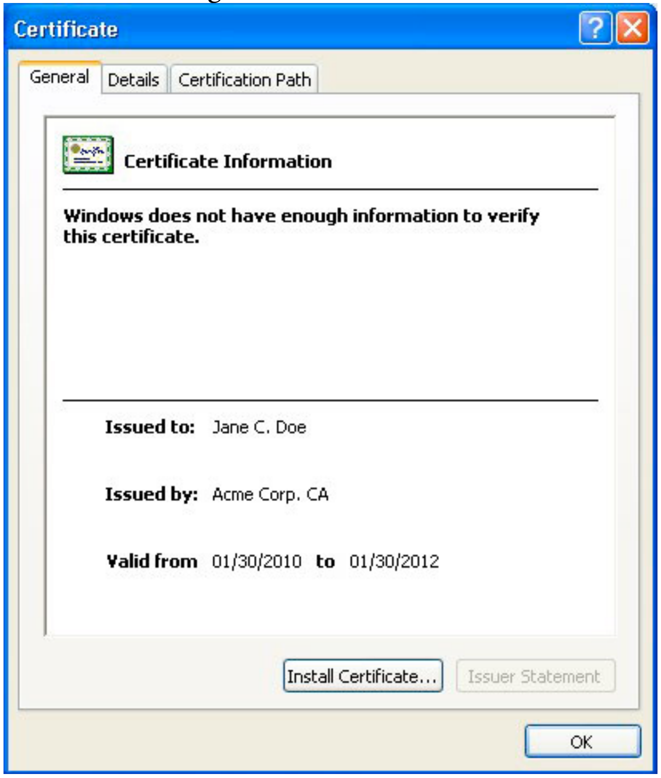

Authentication Certificate
Verify PIN
Change PIN
USB Smart Card Reader - PIV Card
VeriSign Digital ID - Stored on Computer
About VeriSign PKI Client
Exit
4:44 PM

Figure 3.3 - Notification Area Menu

3. Select the Digital ID.
   A Windows Certificate dialog is displayed. In this dialog, you can view basic information about the Digital ID, such as the valid-to date. In the **Details** tab, you can view all information that is stored on the Digital ID.



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: Jane C. Doe

Issued by: Acme Corp. CA

Valid from 01/30/2010 to 01/30/2012

Figure 3.4 - Windows Certificate Dialog

4. After viewing the Digital ID information, click **OK**.

Managing Your PIN

From the notification area, you can verify and change the Personal Identification Number (PIN) for your smart card or Digital ID.

Verifying Your PIN

1. In the Windows notification area, right-click the VeriSign PKI Client icon.
2. In the menu, select the smart card or Digital ID.

3. Select **Verify PIN**.

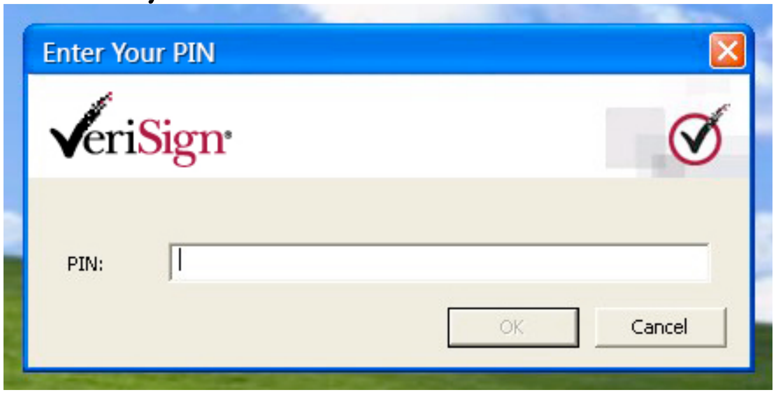


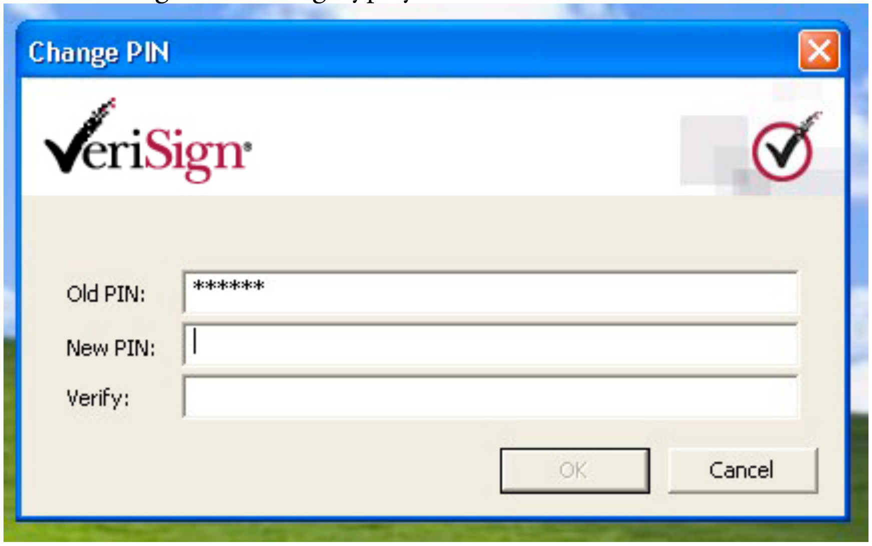
Figure 3.5 - Verify PIN Dialog

4. In the *Enter Your PIN* dialog, type your PIN.
5. Click **OK**. If the PIN you typed is correct, you will receive a success message. If the PIN you typed is incorrect, you will receive an error message and will need to retry.

CAUTION Depending on the smart card or Digital ID you are using, you may only enter an incorrect PIN a few times. If you enter an incorrect PIN too many times, your smart card or Digital ID will be blocked and you will be unable to use it. If you block your PIN, you will either need to be issued a new smart card or have a system administrator unblock your smart card.

Changing Your PIN

1. In the Windows notification area, right-click the VeriSign PKI Client icon.
2. In the menu, select the smart card or Digital ID.
3. Select **Change PIN**.
4. In the Change PIN dialog, type your current PIN.



Old PIN: ******

Figure 3.6 - Change PIN Dialog

5. In the **New PIN** field, type your new PIN.
6. In the **Verify PIN** field, type your new PIN a second time.

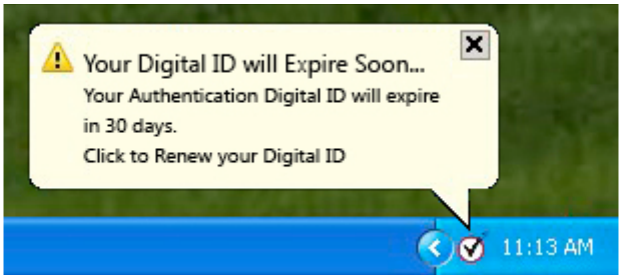
7. Click **OK**.

   If the PIN you typed is correct, you will receive a success message. If the PIN you type is incorrect or your new PINs do not match, you will receive an error message and will need to retry.

CAUTION Depending on the smart card or Digital ID you are using, you may only enter an incorrect PIN a small amount of times. If you enter an incorrect PIN too many times, your smart card or Digital ID will be blocked and you will be unable to use it. If you block your PIN, you will either need to be issued a new smart card or have a system administrator unblock your smart card.

Renewing Expiring Digital IDs

When your Digital ID is close to expiring, you will receive a message in the Windows notification area. When you click this message, your Digital ID will be automatically renewed or you will be taken to a web site to complete the renewal.



Your Digital ID will Expire Soon...

Your Authentication Digital ID will expire in 30 days.

Click to Renew your Digital ID

Figure 3.7 - Renew Digital ID Message

4 Sending Secure Email

You can both digitally sign and encrypt emails in Microsoft Outlook with your Digital ID. Your digital signature allows other people to verify that you sent them an email message and that the message has not been altered.

A digital signature alone does not make your message private. To make a message private with Outlook, you can encrypt it, which garbles the message text so no one beside the intended recipient can read it. The intended recipient will decrypt the message with her own Digital ID.

Note For another person to read a message you have encrypted, you will need to exchange Digital IDs with this person. There are several ways to exchange Digital IDs, which are discussed in Microsoft's online help. Contact your system administrator to learn about the people in your organization that you already trust and can exchange secure email messages with.

VeriSign PKI Client will automatically set up Outlook to use your smart card or Digital ID for digital signatures and encryption. When you connect a smart card, Outlook will automatically start using the Digital ID(s) on this card for email security. If you have multiple Digital IDs and would like to specify the Digital ID that Outlook uses for either digital signatures or encryption, read *Choosing Digital IDs for Email Security* at the end of section.

What You Will Need

To use VeriSign PKI Client for secure email, you will need the following:

- Microsoft Outlook 2003 or 2007
- A Digital ID for digital signatures
- A Digital ID for encryption

These Digital IDs will already be stored on your smart card or computer, or you will be requested by your system administrator to enroll for them.

Using Digital Signatures with Outlook

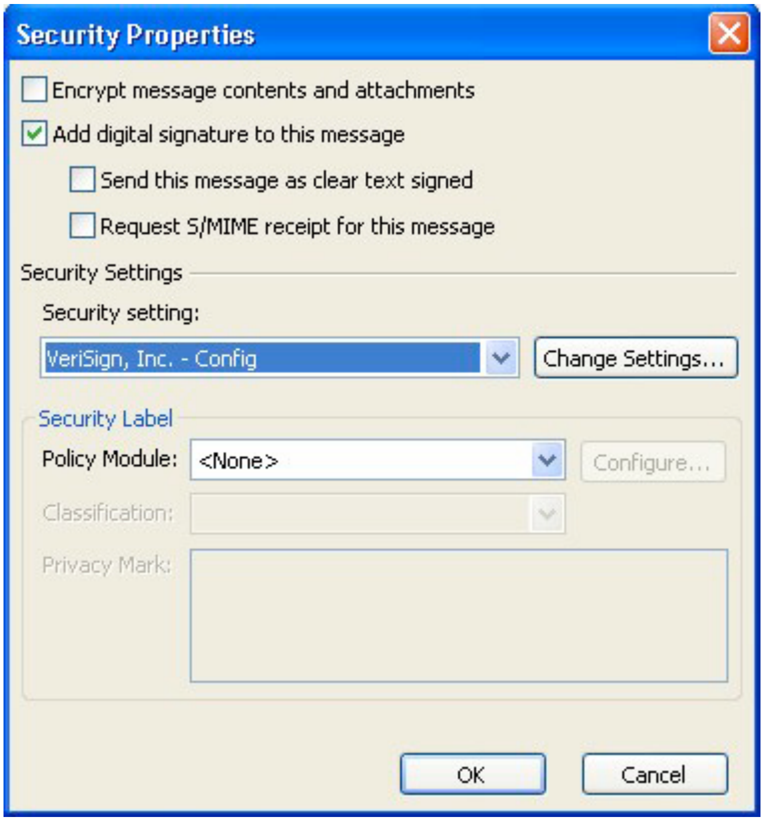
You can digitally sign a single email message or all outgoing email messages.

Digitally Signing a Single Email

The first time you use a digital signature, make sure that the correct Digital ID is used:

1. Open Microsoft Outlook.
2. Create a new email message.
3. Open the *Message Options* dialog:
   - If you are using Outlook 2003, click Options, ▤, in the message window.
   - If you are using Outlook 2007, click the expand icon, ↘, in the Options section of the Message menu.
4. In the *Message Options* dialog, click **Security Settings**.

5. Click the **Add digital signature to this message** check box.
6. In the *Security setting* select box, select the **VeriSign, Inc. - Config** option.



Security Properties

□ Encrypt message contents and attachments

☑ Add digital signature to this message

□ Send this message as clear text signed

□ Request S/MIME receipt for this message

Security Settings

Security setting: VeriSign, Inc. - Config

Security Label

Policy Module: <None>

Figure 4.1 - Message Security Settings

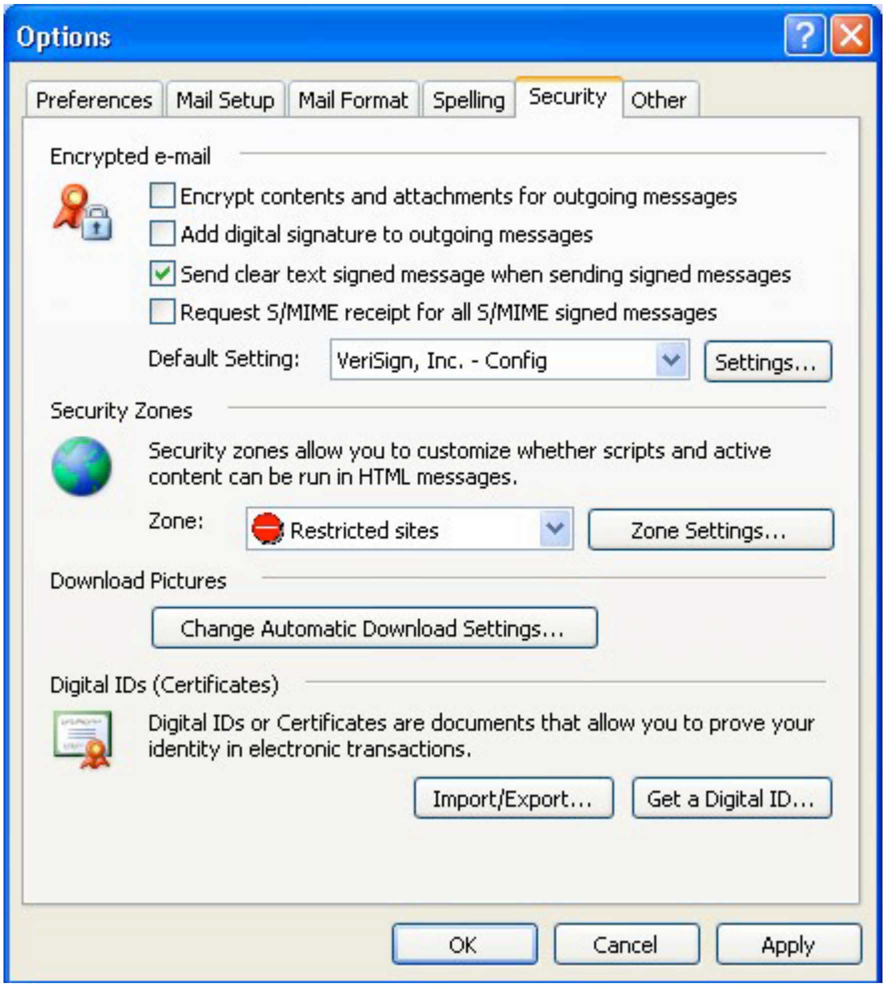
7. Click **OK**.
8. Click **Close** in the *Message Options* dialog.
9. Compose your email message and then send it.
10. When prompted, enter your PIN.

For subsequent emails you can just click the sign icon:

1. Open Microsoft Outlook.
2. Create a new email message.
3. Click the Digitally Sign Message icon, ✉.
4. Compose your email message and then send it.

Digitally Signing All Outgoing Email

1. Open Microsoft Outlook.
2. Open the email security settings:
   - If you are using Outlook 2003, select **Options** in the *Tools* menu. Then click the **Security** tab.
   - If you are using Outlook 2007, select **Trust Center** in the *Tools* menu. Then click **Email Security** in the left panel.
3. In the *Encrypted e-mail* section, click the **Send clear text signed message when sending signed messages** check box.



Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages

□ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: VeriSign, Inc. - Config

Security Zones

Security zones allow you to customize whether scripts and active content can be run in HTML messages.

Zone: Restricted sites

Download Pictures

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Figure 4.2 - Security Options

4. In the *Default Setting* box, select **VeriSign, Inc. - Config**.
5. Click **OK**.

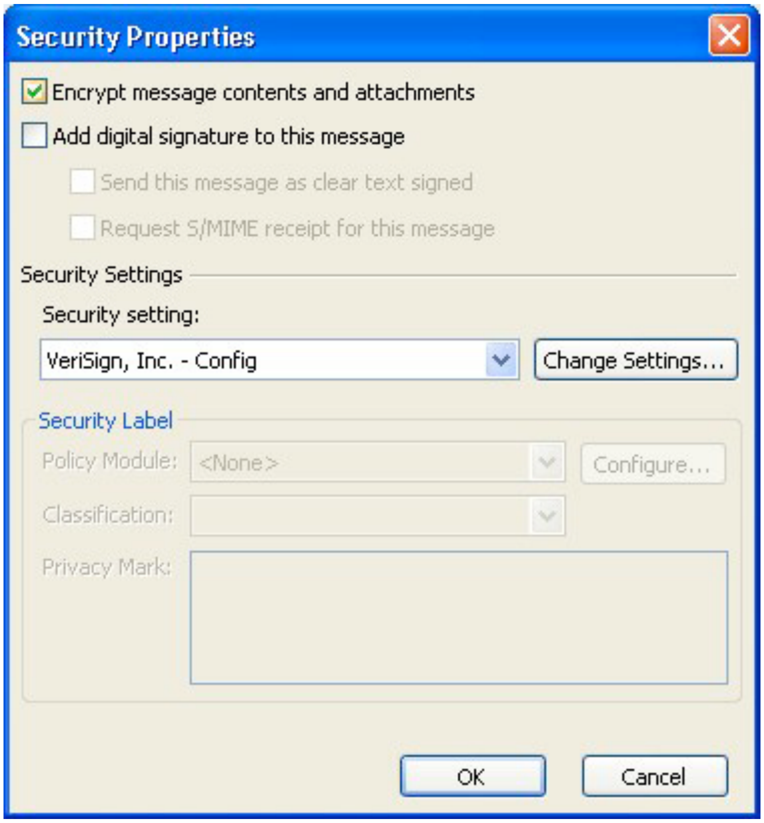
Using Encryption with Outlook

You can enable encryption for a single email message or all outgoing messages.

Encrypting a Single Email

The first time you encrypt an email, make sure that the correct Digital ID is used:

1. Open Microsoft Outlook.
2. Create a new email.
3. Open the *Message Options* dialog:
   - If you are using Outlook 2003, click Options, , in the message window.
   - If you are using Outlook 2007, click the expand icon, , in the Options section of the Message menu.
4. In the *Message Options* dialog, click **Security Settings**.
5. Click the **Encrypt message contents and attachments** check box.
6. In the *Security setting* select box, select the **VeriSign, Inc. - Config** option.



Security Properties

☑ Encrypt message contents and attachments

□ Add digital signature to this message

□ Send this message as clear text signed

□ Request S/MIME receipt for this message

Security Settings

Security setting: VeriSign, Inc. - Config

Security Label

Policy Module: <None>

Classification:

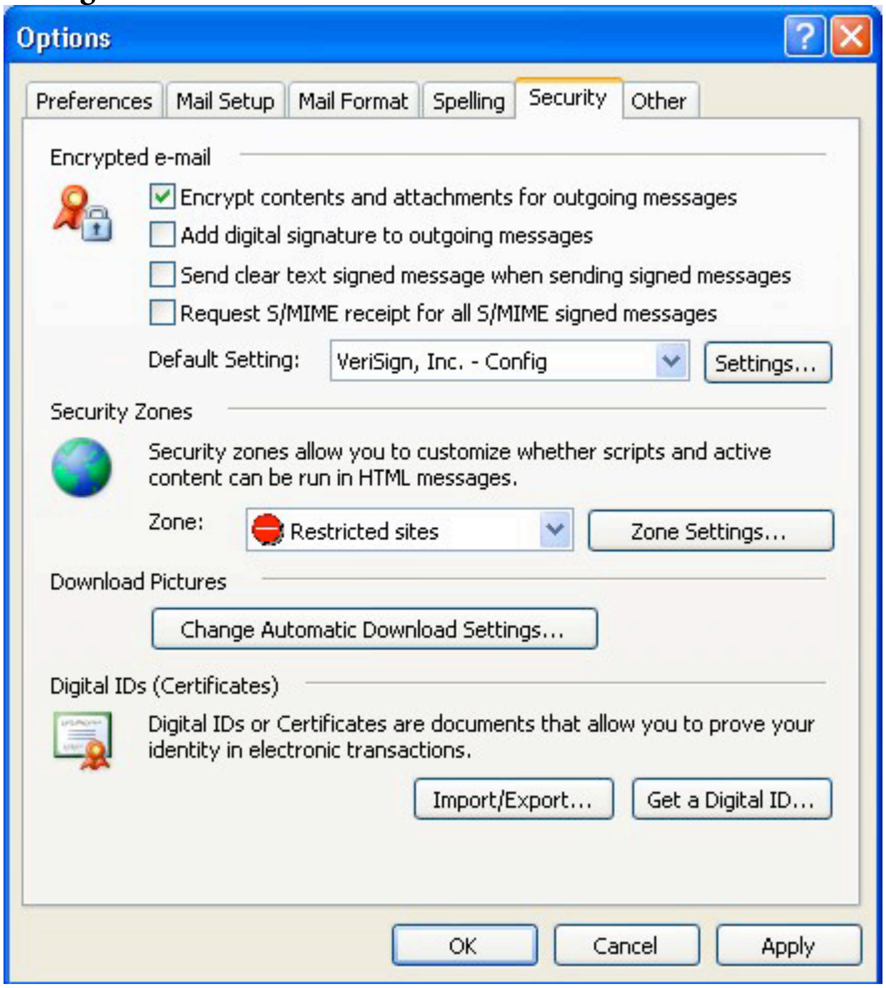
Privacy Mark:

Figure 4.3 - Message Security

7. Click **OK**.
8. Click **Close** in the *Message Options* dialog.
9. Compose your email message and then send it.
10. When prompted, enter your PIN.

Encrypting All Outgoing Email

1. Open Microsoft Outlook.
2. Open the email security settings:
   - If you are using Outlook 2003, select **Options** in the **Tools** menu. Then click the **Security** tab.
   - If you are using Outlook 2007, select **Trust Center** in the **Tools** menu. Then click **Email Security** in the left panel.
3. In the Encrypted e-mail section, click the **Encrypt contents and attachments for outgoing messages** check box.



Encrypted e-mail

☑ Encrypt contents and attachments for outgoing messages

☐ Add digital signature to outgoing messages

☐ Send clear text signed message when sending signed messages

☐ Request S/MIME receipt for all S/MIME signed messages

Default Setting: VeriSign, Inc. - Config

Security Zones

Security zones allow you to customize whether scripts and active content can be run in HTML messages.

Zone: Restricted sites

Download Pictures

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

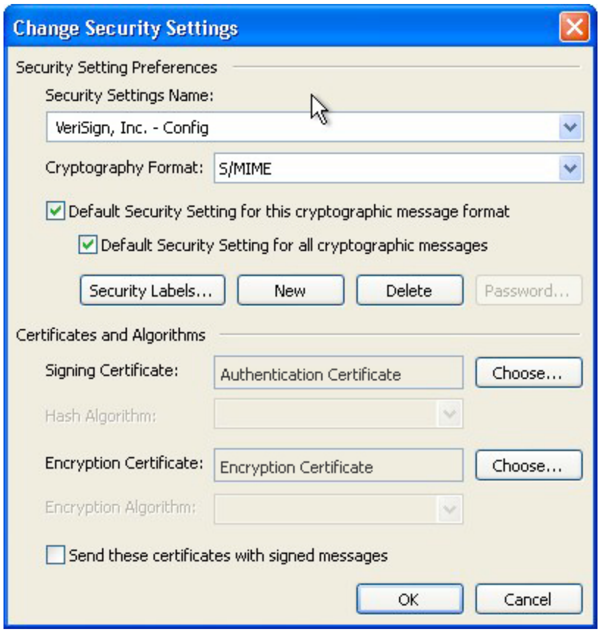
Figure 4.4 - Encrypt All Email Messages

4. In the **Default Setting** box, select "VeriSign, Inc. - Config."
5. Click **OK**.

Choosing a Digital ID for Email Security

If you have multiple Digital IDs for email signing or encryption, you can select the Digital ID that is used in the Microsoft Outlook settings:

1. Open Microsoft Outlook.
2. Open the email security settings:
    - If you are using Outlook 2003, select **Options** in the *Tools* menu. Then click the **Security** tab.
    - If you are using Outlook 2007, select **Trust Center** in the *Tools* menu. Then click **Email Security** in the left panel.
3. In the *Encrypted e-mail* section, click **Settings**.
   In the *Certificates and Algorithms* section you will see the signing and encryption certificates that are being used.



Security Settings Name: VeriSign, Inc. - Config

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Signing Certificate: Authentication Certificate

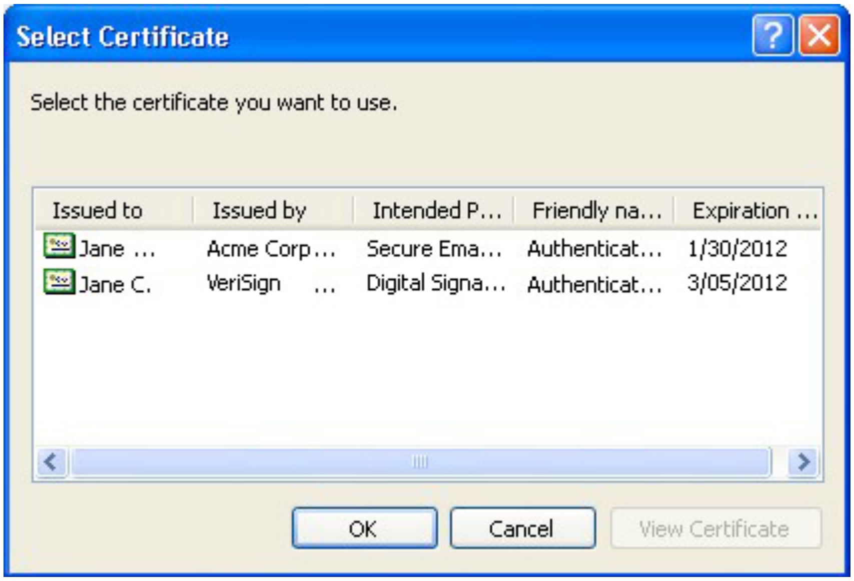
Encryption Certificate: Encryption Certificate

☐ Send these certificates with signed messages

Figure 4.5 - Certificate and Algorithms

4. Click **Choose** in either the **Signing Certificate** or **Encryption Certificate** field.

   All Digital IDs that are available for use for signing and encryption will be shown.



Select the certificate you want to use.

Issued to	Issued by	Intended P…	Friendly na…	Expiration …
Jane …	Acme Corp…	Secure Ema…	Authenticat…	1/30/2012
Jane C.	VeriSign …	Digital Signa…	Authenticat…	3/05/2012

Figure 4.6 - Select Certificate

5. Select the Digital ID you would like to use.
6. Click **OK** in each of the open dialogs.

5 Using Smart Card Log on

Each time you log on to Windows, you can use your PIV or CAC smart card for logon instead of a username and password. Smart card log on may be required by your organization.

You can log on to Windows using your PIV or CAC smart card.

What You Will Need

To use VeriSign PKI Client for Windows logon, you will need:

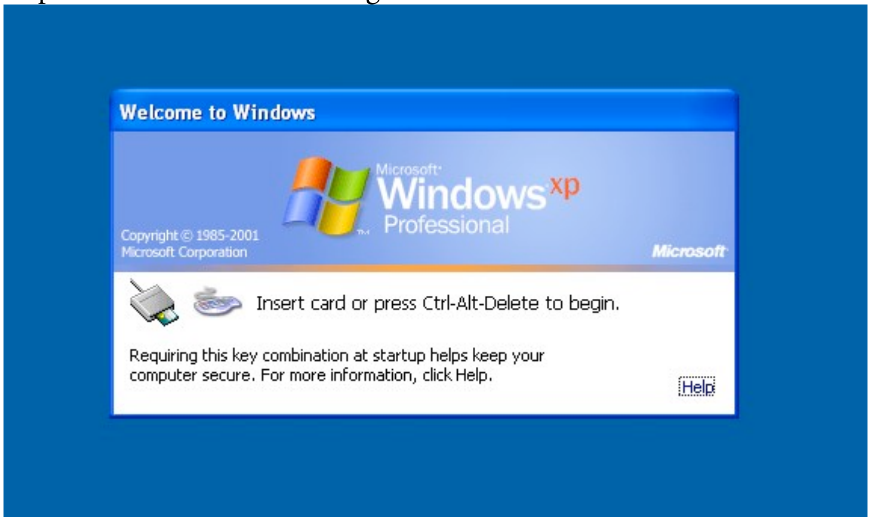
- To be a member of your organization's domain
- A PIV or CAC smart card
- A Digital ID for smart card logon

You will need to be a member of your organization's domain, which should be configured by your system administrator. This Digital ID will already be stored on your smart card, or you will be requested by your system administrator to enroll for it.

Logging on to Windows

1. Logout or restart Windows.

   At the Windows logon screen, you should see instructions for using your smart card: Insert card or press Ctrl-Alt-Delete to begin.



Welcome to Windows

Insert card or press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 5.1 - Insert Smart Card

2. Insert your smart card.

3. Enter your PIN.

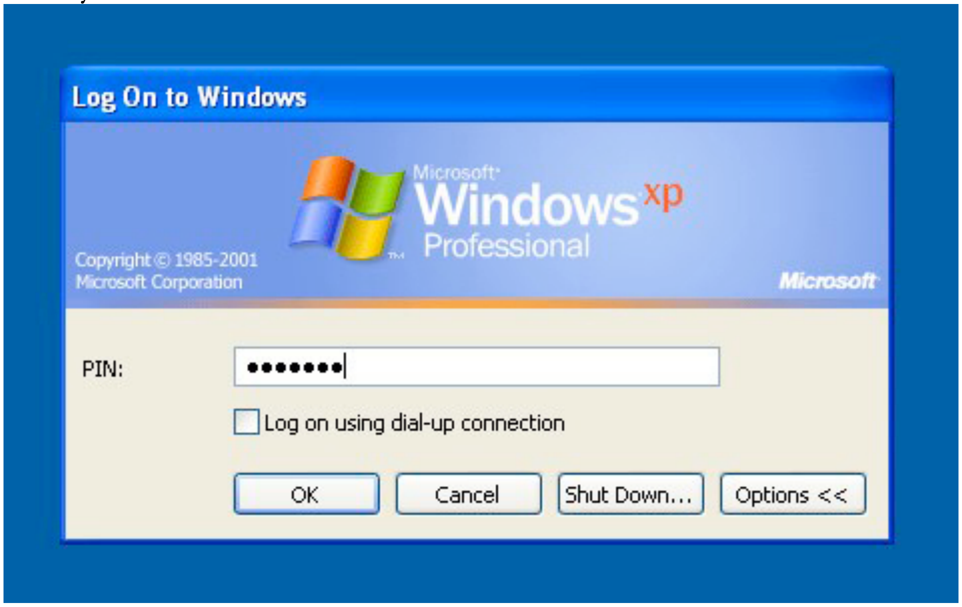


Figure 5.2 - Enter PIN

4. Click **OK**.

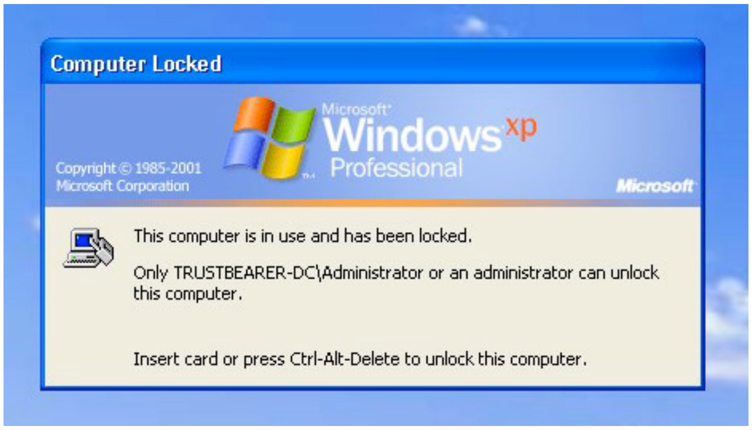
6 Locking and Unlocking Your Computer

Your organization may require that your screen be automatically locked whenever you remove your smart card, and your system administrator will have set this up on your computer.

You will need to have a PIV or CAC smart card and be a member of your organization's domain.

Locking Your Computer

When you remove your smart card from your computer's smart card reader, your screen will be automatically locked.



Computer Locked

This computer is in use and has been locked.

Only TRUSTBEARER-DC\Administrator or an administrator can unlock this computer.

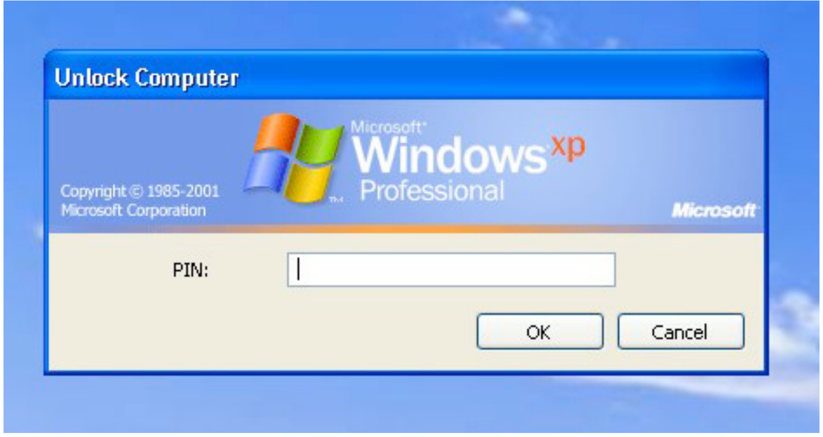
Insert card or press Ctrl-Alt-Delete to unlock this computer.

Figure 6.1 - Computer Locked

Unlocking your Computer

To unlock your computer:

1. Insert your smart card.
2. Enter your PIN.



Unlock Computer

PIN:

Figure 6.2 - Enter PIN

3. Click **OK**.

7 Signing Documents

You can digitally sign portable document format (PDF) documents with Adobe Reader and Adobe Acrobat Professional using your Digital ID. Your digital signature allows other people to verify that you created or made changes to a document, and allows them to see if the document has been altered since you signed it.

What You Will Need

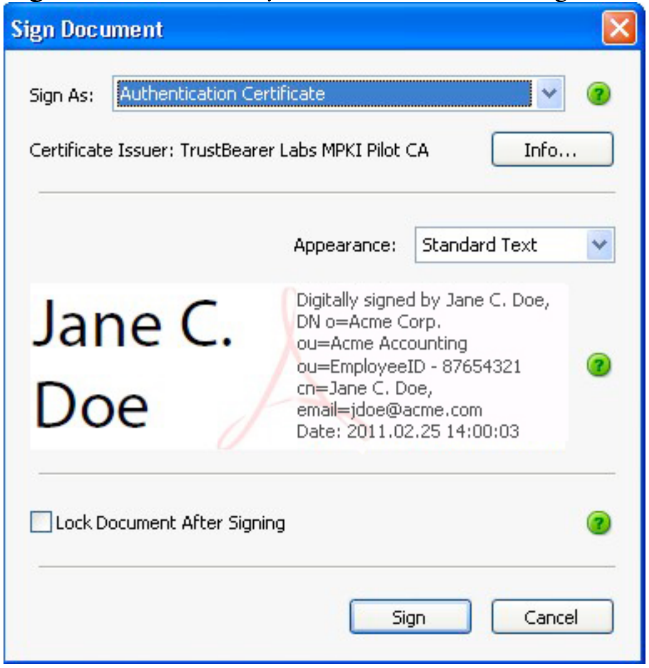
To use VeriSign PKI Client to digitally sign PDF documents, you will need the following:

- Adobe Reader or Adobe Acrobat Professional
- A Digital ID for digital signatures

This Digital ID will already be stored on your smart card or computer, or you will be requested by your system administrator to enroll for it. If you are using Adobe Reader, the original creator of the PDF will need to have enabled digital signing of the document.

Signing Documents in Adobe Reader

1. Open Adobe Reader or Adobe Acrobat Professional.
2. Open the PDF that you will be signing.
3. Select **Sign** > **Sign Document** in the **Document** menu.
4. Click **OK** in the Adobe Reader dialog.
5. Click and draw a window where you would like to place the signature.
   The *Sign Document* dialog will appear and should show the Digital ID you use for signing in the **Sign As** box. You may also select another Digital ID at this time.



Sign Document

Sign As: Authentication Certificate

Certificate Issuer: TrustBearer Labs MPKI Pilot CA

Appearance: Standard Text

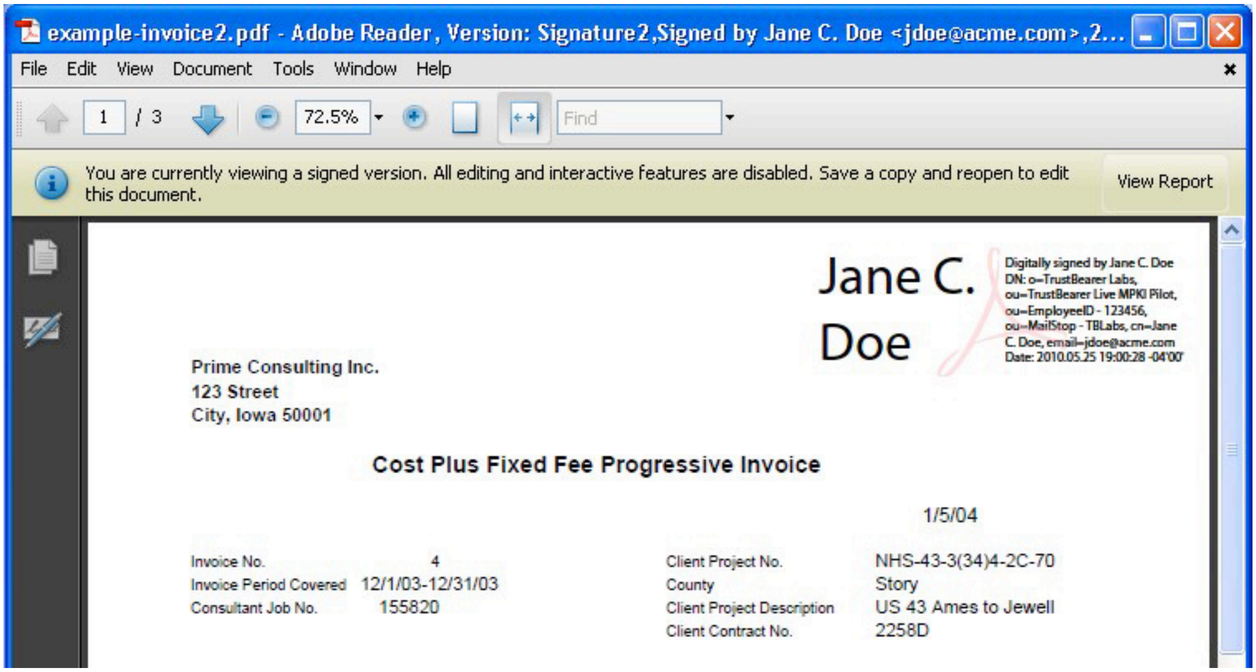
Jane C. Doe

Digitally signed by Jane C. Doe,
DN o=Acme Corp.
ou=Acme Accounting
ou=EmployeeID - 87654321
cn=Jane C. Doe,
email=jdoe@acme.com
Date: 2011.02.25 14:00:03

□ Lock Document After Signing

Figure 7.1 - Sign Document

6. Click **Sign**.
7. In the *Save As* dialog, save the document as a copy or replace the existing file and click **Save**.
8. When prompted, enter your Digital ID PIN.
   You will see the signature on the saved PDF. Similarly other people who view the PDF will see your signature and a message explaining that the document has been signed.


example-invoice2.pdf - Adobe Reader, Version: Signature2,Signed by Jane C. Doe <jdoe@acme.com>,2...
File
Edit
View
Document
Tools
Window
Help
1
/ 3
72.5%
Find
View Report

You are currently viewing a signed version. All editing and interactive features are disabled. Save a copy and reopen to edit this document.

Jane C. Doe

Digitally signed by Jane C. Doe
DN: o=TrustBearer Labs, ou=TrustBearer Live MPKI Pilot, ou=EmployeeID - 123456, ou=MailStop - TBLabs, cn=Jane C. Doe, email=jdoe@acme.com
Date: 2010.05.25 19:00:28 -04'00'

Prime Consulting Inc.
123 Street
City, Iowa 50001

Cost Plus Fixed Fee Progressive Invoice

1/5/04

Invoice No.	4	Client Project No.	NHS-43-3(34)4-2C-70
Invoice Period Covered	12/1/03-12/31/03	County	Story
Consultant Job No.	155820	Client Project Description	US 43 Ames to Jewell
		Client Contract No.	2258D

Figure 7.2 - Signed PDF

8 Using Virtual Private Networks

Virtual Private Network (VPN) technologies allow you to securely connect to a private company network from a remote location on the Internet. For example, you can securely connect to your home office from an insecure hotel WI-FI connection.

What You Will Need

- Cisco VPN Client
- A Virtual Private Network (VPN) Digital ID

Setting Up Cisco VPN Client

You or your system administrator will need to set up Cisco VPN Client with the correct connection settings, including host and connection information.

1. From the *Start* menu, open Cisco VPN Client.
2. Select **Advanced Mode** from the *Options* menu.

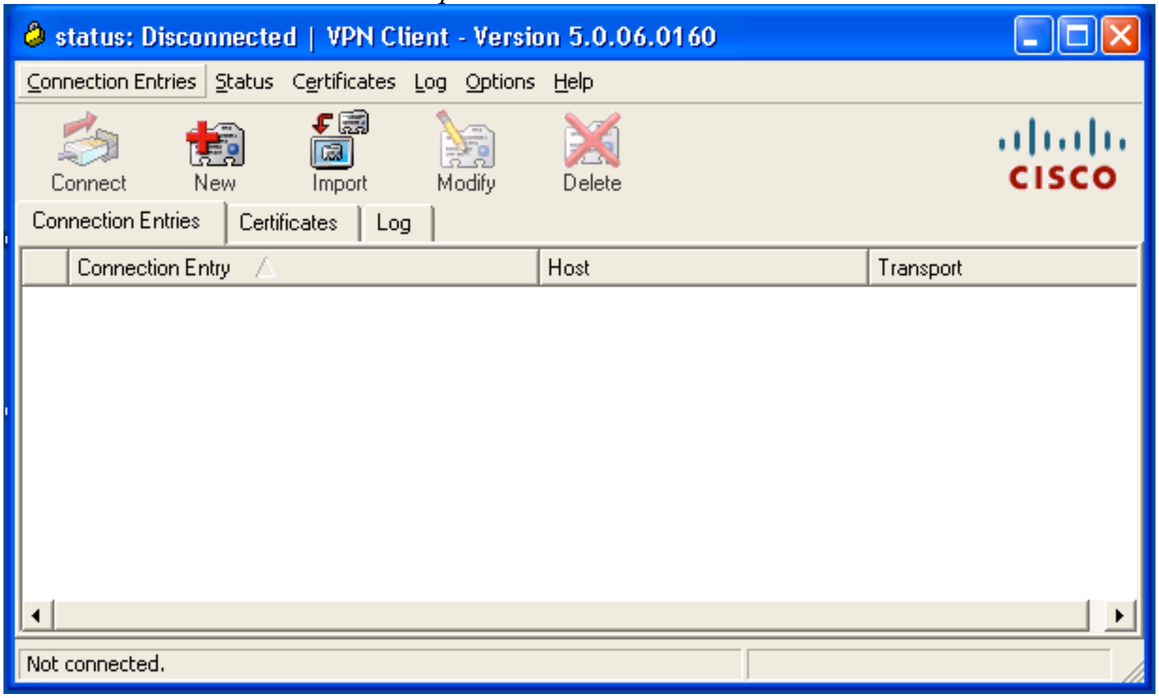
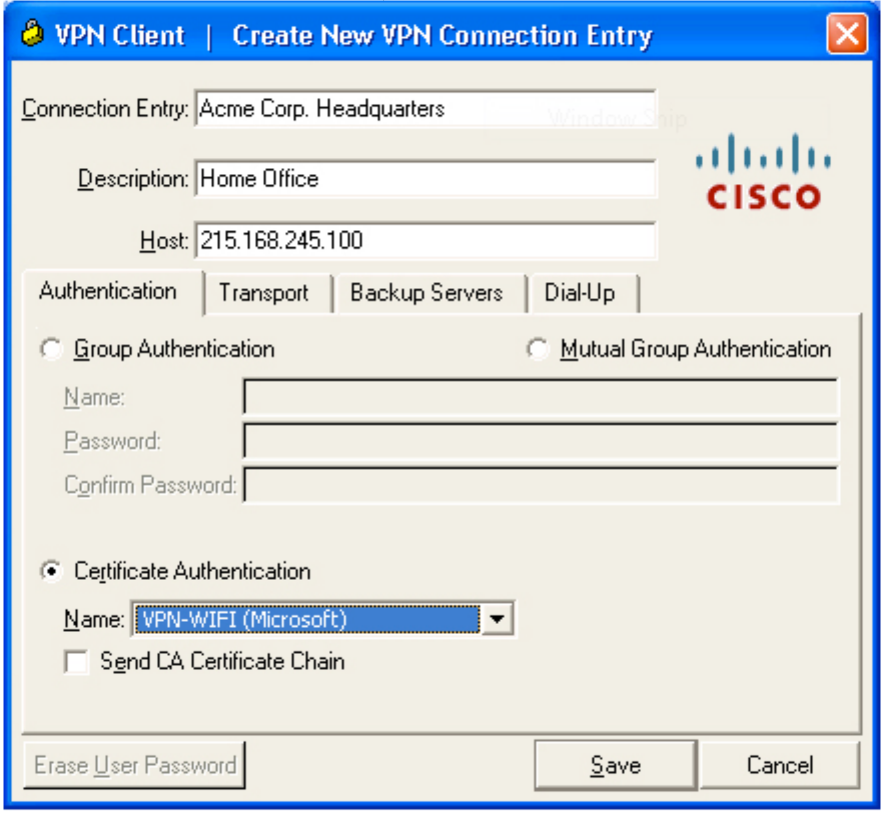


Figure 8.1 - Cisco VPN Client in Advanced Mode

3. From the *Connection Entries* menu, select **New**.
4. Type a unique name in the **Connection Entry** field.
5. Type a name in the **Description**.
6. In the **Host** field, enter the hostname or IP address of the location you will access.
7. Click the **Certificate Authentication** radio option.

8. In the **Name** select box, select your VPN certificate.



VPN Client | Create New VPN Connection Entry

Connection Entry: Acme Corp. Headquarters

Description: Home Office

Host: 215.168.245.100

○ Group Authentication ○ Mutual Group Authentication

Name:

Password:

Confirm Password:

● Certificate Authentication

Name: VPN-WIFI (Microsoft)

□ Send CA Certificate Chain

Figure 8.2 - Cisco VPN Client Connection Settings

9. Click **Save**.
10. Right-click the new connection entry and select **Connect**.

9 Accessing Secure Web Sites

You use Secure Socket Layer (SSL) technology whenever you visit a secure (https) web site. Just as your web browser tells you whether or not a web site should be trusted, you can use SSL to prove your identity to a web site.

Your organization may have an Internet or intranet web site that requires you to authenticate with a SSL Digital ID.

What You Will Need

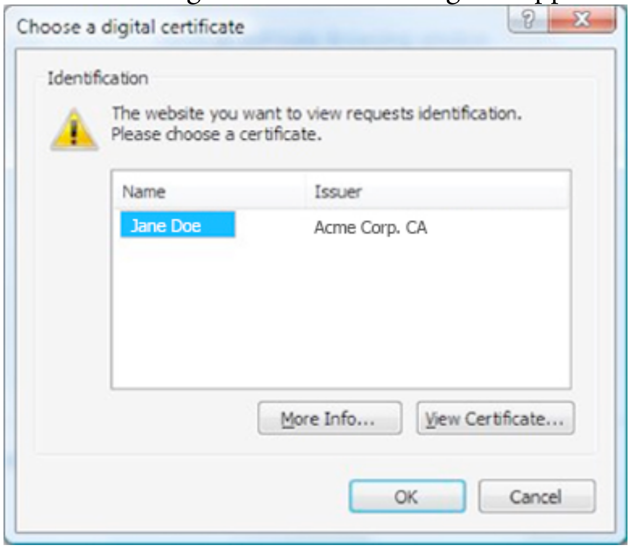
You will need an SSL or Authentication Digital ID. This Digital ID will already be stored on your smart card or computer, or you will be requested by your system administrator to enroll for this Digital ID.

Authenticating to a Web site with Internet Explorer

When you visit a web site that requires SSL authentication, you will present your Digital ID:

1. Open Internet Explorer.
2. Enter the URL for the web site you will be accessing.

   A Choose a Digital Certificate dialog will appear.



Choose a digital certificate

Identification

The website you want to view requests identification. Please choose a certificate.

Name	Issuer
Jane Doe	Acme Corp. CA

Figure 9.1 - Select Digital ID for SSL

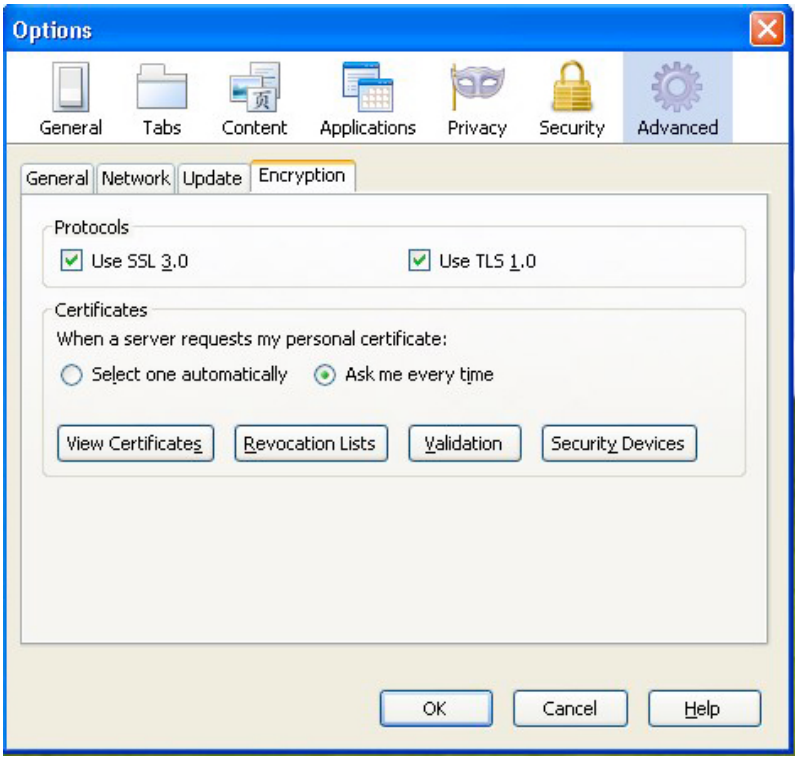
3. From the list of Digital IDs, select your SSL/Authentication Digital ID.
4. Click **OK**.

   After you have selected the Digital ID you may be asked to enter your PIN. After you enter your PIN, the web site will be displayed.

Setting Up Web Authentication with Firefox

If you will be visiting a web site that requires SSL authentication with Mozilla Firefox, you need to configure Firefox to use VeriSign's software for smart cards:

1. Open Mozilla Firefox.
2. Open the Firefox Options dialog (Tools > Options).
3. Select the Advanced section.



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

Figure 9.2 - Firefox Advanced Options

4. Click the **Encryption** tab.

5. Click **Security Devices**.

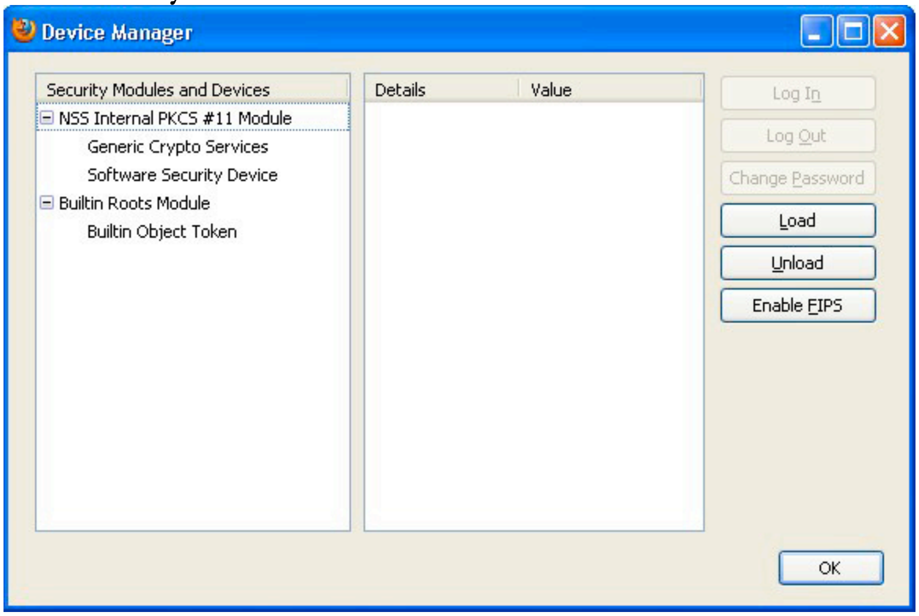
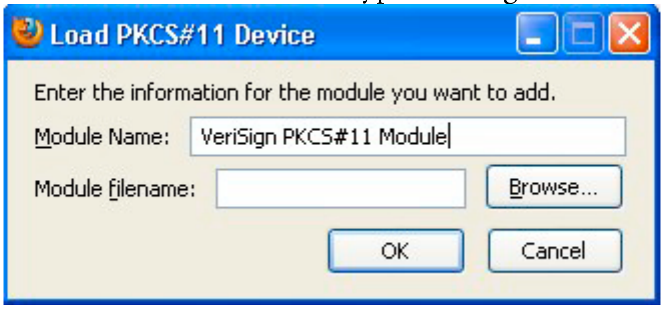


Figure 9.3 - Firefox Device Manager

6. In the Device Manager dialog, click **Load**.
7. In the **Module Name** field, type "VeriSign PKCS#11 Module”



Enter the information for the module you want to add.

Module Name: VeriSign PKCS#11 Module

Module filename:

Figure 9.4 - Firefox Device Manager

8. Click **Browse**.
9. Browse to the VeriSign PKI Client program files (C:\Program FilesVeriSign\PKI Client).

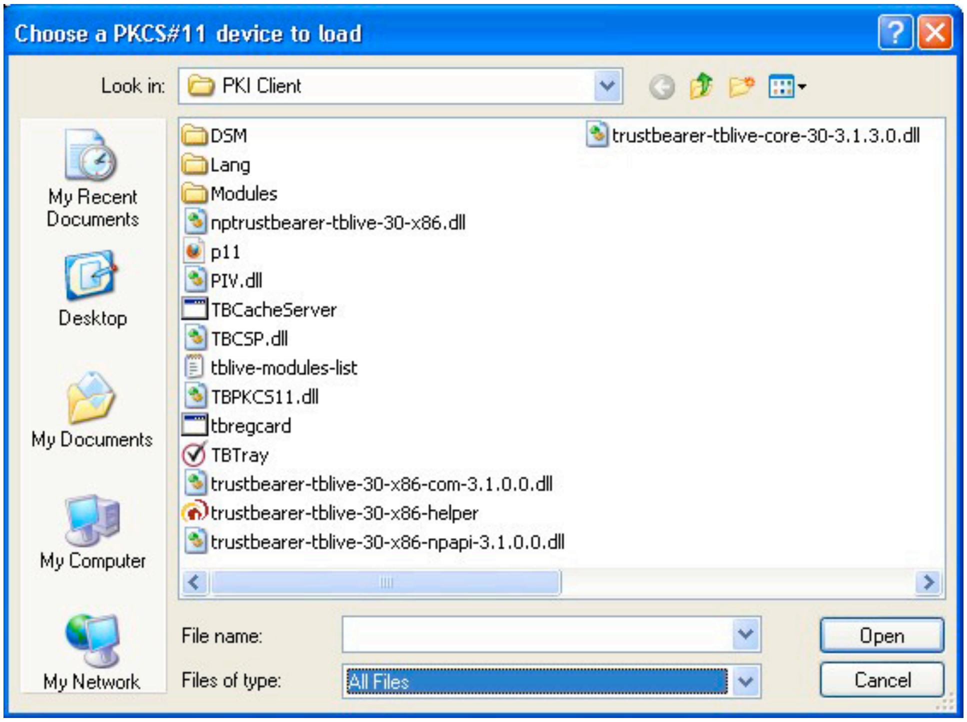

Choose a PKCS#11 device to load
Look in:
PKI Client
My Recent Documents
Desktop
My Documents
My Computer
My Network
DSM
Lang
Modules
nptrustbearer-tblive-30-x86.dll
p11
PIV.dll
TBCacheServer
TBCSP.dll
tblive-modules-list
TBPKCS11.dll
tbregcard
TBTray
trustbearer-tblive-30-x86-com-3.1.0.0.dll
trustbearer-tblive-30-x86-helper
trustbearer-tblive-30-x86-npapi-3.1.0.0.dll
trustbearer-tblive-core-30-3.1.3.0.dll
File name:
Files of type:
All Files
Open
Cancel

Figure 9.5 - VeriSign PKI Client Program Files

10. Select the file named "TBPKCS11.dll”
11. Click **Open**.

There will now be a new listing in the Security Modules and Devices list, which will include your smart card or Digital ID.

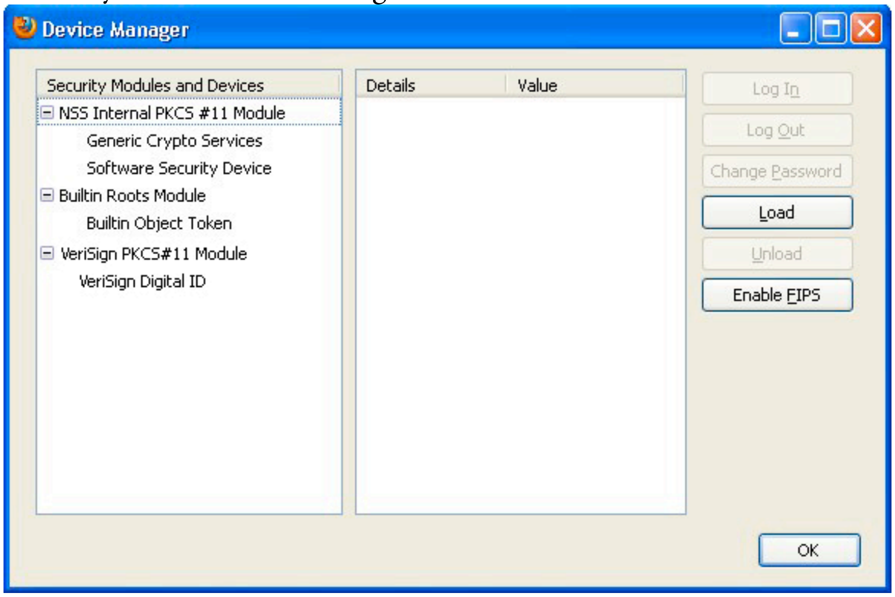


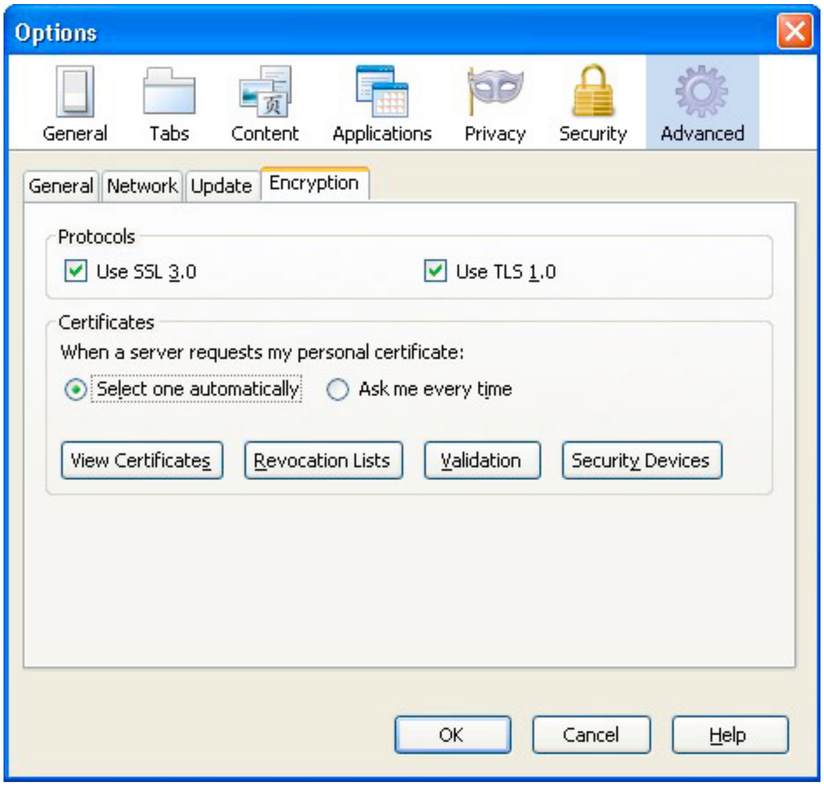
Figure 9.6 - VeriSign PKCS#11 Module Listed

12. Click **OK** in the Load PKCS#11 Device dialog.

13. Click **OK** in the Device Manger dialog.
14. Click **OK** in the Options dialog.

Your Digital ID will now be ready for use with Firefox. You can have Firefox automatically select this Digital ID (Otherwise, Firefox will prompt you to select it when you visit a web site that requires SSL authentication):

1. Open Mozilla Firefox.
2. Open the Firefox Options dialog (Tools > Options).
3. Select the Advanced section.
4. Click the **Encryption** tab.
5. In the Certificates section, click the **Select one automatically** radio option.



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

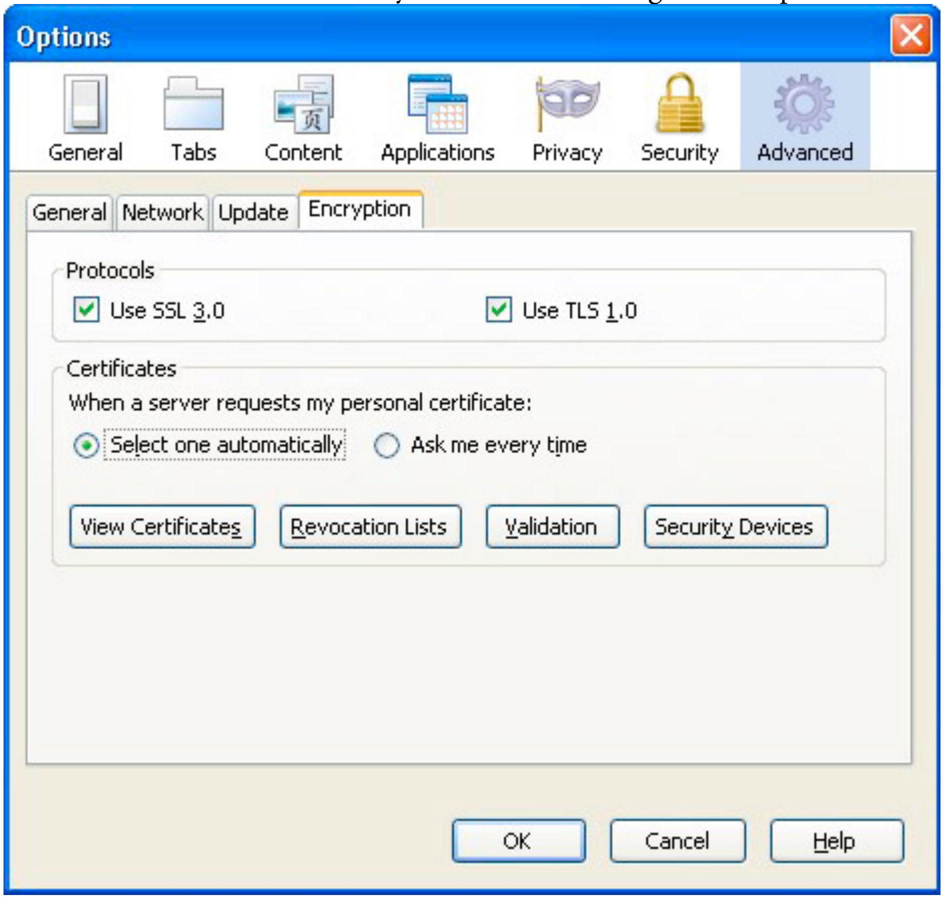
Certificates

When a server requests my personal certificate:

● Select one automatically ○ Ask me every time

Figure 9.7 - Automatically Select Digital ID

6. Click **View Certificates** to verify that the correct Digital ID is present.



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

● Select one automatically ○ Ask me every time

Figure 9.7 - Firefox SSL Certificates

7. Click **OK** in the Certificate Manager dialog.
8. Click **OK** in the Options dialog.